IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Susana Fernandez-Alonso, et al.	§	Group Art Unit:	2617
Application No.	10/595,496	§	Examiner:	Lebassi, Amanuel
Filed:	November 27, 2006	§	Confirmation No:	1578

Attorney Docket No: P18123-US1
Customer No.: 27045

For: Means And Method For Controlling Service Progression Between Different Domains

Via EFS-Web

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313.1450

CERTIFICATE OF TRANSMISSION BY EFS-WEB

Date of Transmission:

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Date: **October 21, 2010**

Name: **Kara Coffman**

Signature: /Kara Coffman/

APPEAL BRIEF

This Appeal Brief is submitted in connection with the decision of the Examiner set forth in an Advisory Action dated July 16, 2010, finally rejecting claims 1, 3-16, 18-25, 27-31, which are all of the pending claims in this application.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §41.20(b)(2) that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1379.

TABLE OF CONTENTS

Real Party in Interest

The real party in interest, by assignment, is:

Telefonaktiebolaget LM Ericsson (publ)
SE-164 83
Stockholm, Sweden

Related Appeals and Interferences

None.

Jurisdictional Statement

The Board has jurisdiction under 35 U.S.C. 134(a). The Examiner mailed a Final Rejection on April 27, 2010, setting a three-month shortened statutory period for response. A response to the Final Rejection was filed on June 25, 2010. The Examiner mailed an Advisory Action on July 16, 2010. The Notice of Appeal was filed on August 25, 2010. The Appeal Brief is being filed before October 26, 2010.

Table of Authorities

Authority	Page in which authority is relied upon
KSR International Co. v. Teleflex Inc.	8

Status of Claims

Claims 1, 3-16, 18-25 and 27-31 are pending in the present application, each of which are finally rejected and form the basis for this Appeal. Claims 1, 3-16, 18-25 and 27-31, including all amendments to the claims thereto are attached in the Claims Appendix.

Status of Amendments

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the Advisory Action.

Summary of Claimed Subject Matter

Claim Element	Specification Reference
1. An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2

service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, and including:	
means for obtaining an authorization decision on whether the user is allowed to access the service;	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2
the Application Gateway Module comprising:	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2
means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2
means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 3A
means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier; and	Throughout the specification, including: paragraph [0017], original claim 2, and FIG. 2, item 2
means for activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2

Claim Element	**Specification Reference**
15. An Authorization Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Authorization Module arranged for deciding whether a user is allowed to access a service and having:	Throughout the specification, including: paragraph [0022], original claim 15, and FIG. 2, item 3

means for receiving a service authorization request from an Application Gateway Module; and	Throughout the specification, including: paragraph [0022], original claim 15, and FIG. 2, item 3
means for returning to the Application Gateway Module a response on whether the user is granted access to the requested service;	Throughout the specification, including: paragraph [0022], original claim 15, and FIG. 2, item 3
the Authorization Module comprising :	Throughout the specification, including: paragraph [0022], original claim 15, and FIG. 2, item 3
means for generating a service session identifier intended to correlate those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;	Throughout the specification, including: paragraph [0022], original claim 15, and FIG. 2, item 3
means for configuring a second finite-state machine with a number of statuses intended to identify specific events in service progression, the second finite-state machine usable by the Authorization Module to act over the Application Gateway Module to control the service progression;	Throughout the specification, including: paragraph [0022], original claim 15, and FIG. 3B
means for initiating a specific instance of the second finite-state machine, said specific instance being identified by said service session identifier; and	Throughout the specification, including: paragraph [0023], original claim 17, and FIG. 2, item 3
means for determining service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.	Throughout the specification, including: paragraph [0022], original claim 15, and FIG. 2, item 3

Claim Element	**Specification Reference**
25. A method for authorizing a user of a service network to access a service offered by a service server of a service provider, the user already authenticated by the service network, the server arranged to deliver a service that comprises a plurality of transactions by exchanging a plurality of	Throughout the specification, including: paragraph [0028], original claim 25, and FIG. 5

application messages with the user, the method comprising the steps of:	
obtaining a first authorization decision on whether the user is allowed to access the service;	Throughout the specification, including: paragraph [0028], original claim 25, and FIG. 5
generating and assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;	Throughout the specification, including: paragraph [0028], original claim 25, and FIG. 5
configuring at least one finite-state machine with a number of statuses intended to identify specific events in service delivery, the finite-state machine usable for controlling service progression	Throughout the specification, including: paragraph [0028], original claim 25, and FIG. 5
initiating a specific instance of the at least one finite-state machine, said specific instance being identified by the assigned service session identifier; and	Throughout the specification, including: paragraph [0029], original claim 26, and FIG. 5
activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.	Throughout the specification, including: paragraph [0028], original claim 25, and FIG. 5

Claim Element	**Specification Reference**
31. An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, the Application Gateway Module comprising:	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2
means for obtaining an authorization decision on whether the user is allowed to access the service;	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2
means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2

means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression from a null state, a service authorization state, an active service state, and a disconnect service state; and	Throughout the specification, including: paragraphs [0016] and [0050], original claim 1, and FIGS. 3A and 4
means for activating service policies applicable to said specific events and resulting in a state transition in the first finite-state machine, the activating means further comprising:	Throughout the specification, including: paragraph [0016], original claim 1, and FIG. 2, item 2
means for statically arming at least one of the service policies before arrival of a first message to invoke the service; and	Throughout the specification, including: paragraphs [0055] and [0058], and FIG. 4
means for dynamically arming at least one of the service policies during the progression of the service.	Throughout the specification, including: paragraphs [0055] and [0058], and FIG. 4

The specification references listed above are provided solely to comply with the USPTO's current regulations regarding appeal briefs. The use of such references should not be interpreted to limit the scope of the claims to such references, nor to limit the scope of the claimed invention in any manner.

Grounds of Rejection to be Reviewed on Appeal

The issue presented for this appeal is whether the independent claims 1, 15, 25, and 31* where properly rejected under 35 U.S.C. §103(a) as being unpatentable over Thomas (US 2004/0039827) in view of Lev Ran (US 2004/0255048). The rejection of the dependent claims 3-14, 16, 18-24, 27-30 stand or fall with the independent claims 1, 15, and 25.

*The independent claim 31 was added in the response to the Final Office Action and entered by the Examiner in the Advisory Action.

Argument

The independent claims 1, 15, 25, and 31 are not obvious in view of Thomas and Lev Ran under 35 U.S.C. 103(a)

Claim 1:

The patent law is clear for a claim to be obvious under 35 U.S.C. 103 then all of the claimed elements have to be known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded nothing more than predictable results to one of ordinary skill in the art. KSR International Co. v. Teleflex Inc., 550 U.S. ___,___, 82 USPQ2d 1385, 1395 (2007). In the present case, Applicant respectfully submits that the Examiner has failed to establish a prima facie case of obviousness since the cited references Thomas and Lev Ran at least fail to teach all of the claimed elements. The pending independent claim 1 is as follows:

> 1. An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, and including:
>
> means for obtaining an authorization decision on whether the user is allowed to access the service;
>
> the Application Gateway Module comprising:
>
> means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;
>
> means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression
>
> means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier; and
>
> means for activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

The highlighted claimed elements are not found in either Thomas or Lev Ran.

The presently claimed invention relates to the control of a service progression when a service network authorizes the user to access a service offered by a service provider. In particular, the presently claimed invention solves an underlying problem where a service network operator does not realize when different transactions of a service take place between a user and service provider. Since, the service network operator is not aware of the different actions of a service carried out by a user and a service provider they can not apply specific policies depending on such different actions. Thomas and Lev Ran do not address this technical problem. Instead, Thomas discloses a method and system for providing secure access to private networks with client redirection. Lev Ran relates to computer file systems and specifically to computer file sharing in a distributed network environment. In view of these basic differences, Applicant respectfully submits that it would follow where Thomas and Lev Ran fail to render the pending independent claim 1 as being unpatentable as will be discussed in detail below.

The closest prior art Thomas discloses in paragraphs [0064]-[0067] is an intermediary server and the Examiner interprets this entity as reading-on the claimed Application Gateway Module. Thomas also discloses on paragraph [0259] an LSP intercepting calls, this LSP being part of a Microsoft OS such as Windows for securing communications to or from sockets. In addition, Thomas discloses on [0260] the LSP being part of the intermediary server. The Examiner also interprets this LSP as being part of the claimed Application Gateway Module. However, Thomas does not disclose where the LSP identifies the user and the service from the intercepted messages. Instead, LSP is intended to communicate different applications with Windows sockets and, as such, there is no disclosure where the LSP may identify a user accessing a service in a service network, simply because this is not a task for the LSP service. Thus, the interpretation made by the Examiner that the intermediary server with the LSP reads-on the claimed Application Gateway Module, which is arranged for intercepting application messages between the user and the service and for identifying said user and said service, is thus wrong.

In addition, Thomas discloses on [0073]-[0075] an authentication procedure carried out when the user first tries to login in the system, and when this authentication

is successful, the user is given a session identifier to be presented to access the various resources in the private network through the intermediary server. However, even if Thomas discloses a user authentication, these paragraphs fail to read-on the claimed means for obtaining an authorization decision on whether the user is allowed to access the service, since authentication and authorization are well known to be different techniques.

Furthermore, Thomas discloses on paragraph [0075] providing a session identifier to the requestor as a result of a successful authentication, this session identifier used in subsequent requests to the intermediary server as long as the session is active. Subsequent requests to the intermediary server may correspond to a same or to different services and, generally speaking, is related to the session established between the authenticated user and the intermediary server. As commented above, Thomas discloses on [0073]-[0075] "...the user is given a session identifier to be presented to access the various resources in the private network..." In contrast, the claim 1 recites "assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user", that is, in claim 1 there is one service session identifier for each service delivery so that, where more than one service is delivered within a session, corresponding more than one service session identifiers are assigned. Consequently, the "session identifier used in subsequent requests to the intermediary server as long as the session is active" disclosed on paragraph [0075] of Thomas, even if similarly worded, does not anticipate the "service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user" recited in the pending claim 1.

Thomas also discloses on paragraph [0286] a state machine. In Thomas's disclosure, "the state machine is based on characteristics of the Windsock API and/or communication protocol API can handle the port mapped data". Apart from this paragraph being editorially confusing, this disclosure does not teach "configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite-state machine configured to control service progression".

Of course, any conventional state machine comprises a number of statuses, but it is the intention and function of the statuses and transitions between them which are relevant factors when prosecuting this patent application. In this respect, Thomas fails to disclose statuses intended to identify specific events in service delivery, because APIs are mere descriptions of how communications between layers are carried out, rather than service progression. Moreover, Thomas's paragraphs [0286]-[0287] deal with the selection of loopback addresses and ports involved in the LSP interception (already commented above) and this has nothing to do with the service progression of a service authorized for a user. Consequently, the specific state machine recited in claim 1 is different from the specific state machine disclosed in Thomas, which is at least a non-enabling disclosure.

Still with reference to Thomas's paragraph [0286], and in the light of paragraph [0069] the Examiner contends this disclosure teaches the claimed feature "initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier". As already commented above, Thomas's paragraph [0286] merely discloses "the state machine is based on characteristics of the Windsock API and/or communication protocol API can handle the port mapped data" whereas Thomas's paragraph [0069] discloses the intermediary server including a cookie manager. This cookie manager manages cookies previously received from a remote server and stored until being delivered to the remote server at appropriate times. These cookies are said to be set by a remote server and used for session, state or identification purposes. That is, Thomas discloses on [0069] cookies set by the remote server, submitted from the remote server to the intermediary server (which the Examiner has constructed as the claimed Application Gateway module), stored at the intermediary server, and returned from the intermediary server to the remote server at appropriate times. This teaching does not suggest an "Application Gateway Module having means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier" as recited in claim 1, and by no means can be similarly interpreted even if isolated words like 'state' and 'session' appear in Thomas's paragraph [0069].

In this regard, Thomas's paragraph [0069] does not disclose the Application Gateway Module (intermediary server in the interpretation of the Examiner) having means for initiating a specific instance of the first finite-state machine cited on Thomas's paragraph [0286], since there is no hint to combine cookies received from the remote server with "the state machine is based on characteristics of the Windsock API and/or communication protocol API can handle the port mapped data". Consequently, there is no disclosure or suggestion in view of Thomas's paragraphs [0069] or [0286] of identifying such (undisclosed) specific instance of the state machine by the assigned service session identifier. Therefore, one can unambiguously conclude that Thomas's paragraph [0069] cannot be naturally combined with paragraph [0286] and, even if combined, the paragraphs [0069] and [0286] fail to disclose the claimed "Application Gateway Module having means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier". Moreover, combining the cookies received from a remote server, as disclosed in Thomas's paragraph [0069], with the state machine based on characteristics of the Winsock API, as disclosed in Thomas's paragraph [0286], does not make any technical sense for any person skilled in the art that uses cookies as identifiers and follows API's for communication between different applications or application layers.

Further, the Examiner refers to the secondary reference Lev Ran to "find" a citation of "activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier", which the Examiner recognizes is not disclosed in the closest prior art Thomas. At this point, the Examiner should recognize that the claimed specific events are related to statuses of the finite-sate machine, as already commented above, and that the claimed service policies applied to the specific events result in state transitions in the specific instance identified by the assigned service session identifier.

However, Lev Ran's paragraph [0204], which has been specifically cited by the Examiner, discloses "Recurrence is a time property that can be applied to all directives. For example, discrete-time directive, such as for pre-positioning, can be activated every day at midnight. Similarly, a continuous-time directive, such as for a cache policy, can

be activated every day between 9:00 a.m. and 5:00 p.m. Preferably, the recurrence granularity ranges from minutes (smallest) to years (largest)". This teaching discloses activation of recurrent directives, in particular for a cache policy, and nothing more than that. This teaching neither discloses nor suggests applying service policies to specific events related with statuses of a finite-state machine, and resulting in a state transition in the specific instance of the finite-state machine identified by the assigned service session identifier.

The Examiner has not substantiated why the skilled person aware of the activation of recurrent directives would have arrived to provide the claimed "activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier". Even if the Examiner, with a broad interpretation, might arrive to identify the "activation of recurrent directives" in Lev Ran with the "activating service policies applicable to said specific events" in claim 1, there is no motivation or suggestion for arriving to "the applied policies resulting in a state transition in the specific instance identified by the assigned service session identifier".

In addition, Lev Ran's paragraph [0459], which has been specifically cited by the Examiner in combination with Le Ran's paragraph [0204], discloses addressing and naming principles governing communications between RPC servers and RPC clients. In this respect, Lev Ran's paragraph [0450] discloses that "Remote services are activated by bidirectionally transferring remote procedure call (RPC) messages between a client application transport layer (RPC client) on one VFN gateway and a server application transport layer (RPC server) on a second remote VFN gateway. Following this definition, Lev Ran's paragraph [0459] teaches that, since an application transport layer may provide the same service on several remote servers, and each RPC server may offer more than one service, then an RPC request must identify the remote RPC server to which it is addressed. More specifically, Lev Ran's paragraph [0459] cites using hostnames, or logical names, or path + port, or URN.

As such, Lev Ran's paragraph [0459] does not add any substantial contribution to the teaching in Lev Ran's paragraph [0204] which might be helpful for the skilled parson to arrive at the "activating service policies applicable to said specific events and

resulting in a state transition in the specific instance identified by the assigned service session identifier" as recited in the pending claim 1. Hence, there is no reasonable expectation of success of combining Thomas and Lev Ran. In view of at least the foregoing, Applicant respectfully submits that the independent claim 1 and the corresponding dependent claims 3-14 are patentable over Thomas, Lev Ran, or any combination thereof.

Claim 15

Applicant respectfully traverses the obviousness rejection of independent claim 15 in view Thomas, Lev Ran or any combination thereof. The independent claim 15 is as follows:

> 15. An Authorization Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Authorization Module arranged for deciding whether a user is allowed to access a service and having:
> means for receiving a service authorization request from an Application Gateway Module; and
> means for returning to the Application Gateway Module a response on whether the user is granted access to the requested service;
> the Authorization Module comprising :
> means for generating a service session identifier intended to correlate those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;
> means for configuring a second finite-state machine with a number of statuses intended to identify specific events in service progression, the second finite-state machine usable by the Authorization Module to act over the Application Gateway Module to control the service progression;
> means for initiating a specific instance of the second finite-state machine, said specific instance being identified by said service session identifier; and
> means for determining service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

The highlighted claimed elements are not found in either Thomas or Lev Ran.

The closest prior art Thomas discloses in paragraphs [0058]-[0059] an intermediary server and the Examiner interprets this entity as reading-on the claimed Authorization Module. Thomas's paragraph [0059] discloses client machines accessing

an intermediary server with requests for contents residing at private servers. The intermediary server, once the client machine is authenticated and authorized to get such contents, accesses the private server to obtain the requested contents and returns the contents to the requester client machine. Since, Thomas's intermediary server is interpreted as being both the Authorization Module and the Application Gateway Module in the present patent application, the various communications between these two modules are not considered to be relevant distinguishing features and will not be discussed hereinafter.

However, Thomas's paragraph [0072] discloses the intermediary server storing session identifiers, or cookies, for the clients or requesters. There is no specific teaching in this paragraph on whether a user may have more than one session identifier at a time. More specifically, Thomas's storing session identifiers for the clients does not teach the claimed "means for generating a service session identifier intended to correlate those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user". As already commented above with respect to the claim 1, there is one service session identifier for each service delivery so that, where more than one service is delivered within a session, corresponding more than one service session identifiers are assigned, whereas Thomas does not teach the service session identifier for each service delivery.

Further, the Examiner interprets the teaching in Thomas's paragraph [0286] as teaching the claimed "means for configuring a second finite-state machine with a number of statuses intended to identify specific events in service progression, the second finite-state machine usable by the Authorization Module to act over the Application Gateway Module to control the service progression". This same teaching has been also used to object the first finite-state machine in the Application Gateway Module in the independent claim 1. Consequently, the same rationale used above in respect of Thomas's paragraph [0286] to defend the corresponding distinguishing feature of claim 1 can be used here to defend the second finite-state machine usable by the Authorization Module in claim 15.

Likewise, the Examiner interprets Thomas's paragraph [0069] in combination with paragraph [0286] as reading-on the claimed "means for initiating a specific instance

of the second finite-state machine, said specific instance being identified by said service session identifier". The handling of cookies as disclosed in Thomas's paragraph [0069] has been discussed above with respect to claim 1 and is also applicable here. Consequently, the same rationale used above with respect to Thomas's paragraphs [0069] and [0286] to defend the corresponding distinguishing feature of claim 1 can be used here to defend the specific instance of the second finite-state machine, and identified by the service session identifier included in the Authorization Module under the independent claim 15.

Still further, the Examiner considers the teaching in Lev Ran's paragraphs [0204] and [0459] to read on the claimed "means for determining service policies applicable to said specific events and resulting in the state transition in the specific instance identified by the assigned service session identifier". Consequently, the same rationale used above with respect to Lev Ran's paragraphs [0204] and [0459] to defend the corresponding distinguishing feature of claim 1 can be used here as well to defend the claimed "means for determining service policies applicable to said specific events and resulting in the state transition in the specific instance identified by the assigned service session identifier". In view of at least the foregoing, Applicant respectfully submits that the independent claim 15 and the corresponding dependent claims 16, 18-24 are patentable over Thomas, Lev Ran, or any combination thereof.

Claim 25

Applicant respectfully submits that the pending independent claim 25 is also patentable in view of Thomas, Lev Ran or any combination thereof. The independent claim 25 is as follows:

> 25. A method for authorizing a user of a service network to access a service offered by a service server of a service provider, the user already authenticated by the service network, the server arranged to deliver a service that comprises a plurality of transactions by exchanging a plurality of application messages with the user, the method comprising the steps of:
>
> obtaining a first authorization decision on whether the user is allowed to access the service;
>
> generating and assigning a service session identifier intended to identify those application messages exchanged between the user and the service and

that belong to a same service delivery authorized for said user;

configuring at least one finite-state machine with a number of statuses intended to identify specific events in service delivery, the finite-state machine usable for controlling service progression

initiating a specific instance of the at least one finite-state machine, said specific instance being identified by the assigned service session identifier; and

activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

The independent claim 25 recites the same or similar distinguishing limitations that have been discussed above with respect to the independent claims 1 and 15. As such, the aforementioned remarks regarding the patentability of the independent claims 1 and 15 apply as well to the independent claim 25. Accordingly, Applicant respectfully requests the allowance of the independent claim 25 and the corresponding dependent claims 27-30.

Claim 31

Applicant respectfully submits that the pending independent claim 31 is patentable in view of Thomas, Lev Ran or any combination thereof. The independent claim 31 is as follows:

31. An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, the Application Gateway Module comprising:

means for obtaining an authorization decision on whether the user is allowed to access the service;

means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;

means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression from a null state, a service authorization state, an active service state, and a disconnect service state; and

means for activating service policies applicable to said specific events and resulting in a state transition in the first finite-state machine, the activating means further comprising:

means for statically arming at least one of the service policies before arrival of a first message to invoke the service; and

means for dynamically arming at least one of the service policies during the progression of the service.

The independent claim 31 recites that the claimed means for activating service policies further includes: (1) means for statically arming at least one of the service policies before arrival of a first message to invoke the service; and (2) means for dynamically arming at least one of the service policies during the progression of the service. These new limitations along with limitations that are similar to the ones discussed above with respect to claim 1 clearly distinguishes the present invention over Thomas, Lev Ran or any combination thereof. Thus, Applicant respectfully submits that the independent claim 31 is patentable over Thomas, Lev Ran or any combination thereof.

CONCLUSION

The claims currently pending in the application are patentable over Thomas and Lev Ran, and the Applicants request that the Examiner's rejection thereof be reversed and the application be allowed.

Respectfully submitted,

/William J. Tucker/

By William J. Tucker
Registration No. 41,356

Date: October 21, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(214) 324-7280 or (972) 583-2608
william.tucker@ericsson.com

CLAIMS APPENDIX

1. (Rejected) An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, and including:

means for obtaining an authorization decision on whether the user is allowed to access the service;

the Application Gateway Module comprising:

means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;

means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression

means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier; and

means for activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

2. (Canceled)

3. (Rejected) The Application Gateway Module of claim 1, wherein the means for activating service policies include means for setting at least one element selected from a non-exhaustive list of references and attributes that comprises:

a number of message field values to match, a number of specific actions to carry out on matching, a number of timer values to run, and a number of transactions to supervise.

4. (Rejected) The Application Gateway Module of claim 1, wherein the means for activating service policies include means for activating a global service policy independently of any service delivery in progress.

5. (Rejected) The Application Gateway Module of claim 1, wherein the means for activating service policies include means for initiating an instance of a global service policy to apply as an individual service policy within a specific instance of the first finite-state machine, the individual service policy inheriting references and attributes from the global service policy.

6. (Rejected) The Application Gateway Module of claim 5, further comprising means for overwriting references and attributes of an individual service policy with new references and attributes during a service progression handled within a specific instance of the first finite- state machine.

7. (Rejected) The Application Gateway Module of claim 5, wherein a particular state is associated with a number of individual service policies within a specific instance of the first finite-state machine, said instance identified by a given service session identifier.

8. (Rejected) The Application Gateway Module of claim 1, wherein the means for obtaining an authorization decision include means for requesting a service authorization from an Authorization Module.

9. (Rejected) The Application Gateway Module of claim 8, wherein the means for activating service policies include means for receiving from the Authorization Module at least one element applicable to set a service policy, the element selected from a non-exhaustive list of references and attributes that comprises: a number of message field values to match, a number of specific actions to carry out on matching, a number of timer values to run, and a number of transactions to supervise.

10. (Rejected) The Application Gateway Module of claim 8, wherein the means for activating service policies includes means for receiving a global service policy from the Authorization Module.

11. (Rejected) The Application Gateway Module of claim 8, further comprising means for receiving references and attributes from the Authorization Module applicable to overwrite an individual service policy with new references and attributes during a service progression handled within a specific instance of the first finite-state machine.

12. (Rejected) The Application Gateway Module of claim 8, further comprising means for notifying to the Authorization Module a specific event in service progression.

13. (Rejected) The Application Gateway Module of claim 8, further comprising means for requesting from the Authorization Module a further processing to determine an appropriate action to go on with the service progression.

14. (Rejected) The Application Gateway Module of claim 13, further comprising means for receiving from the Authorization Module an instruction selected from: access granted without restriction, another service to substitute a previous service requested, forced logout, and indication of a state transition.

15. (Rejected) An Authorization Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Authorization Module arranged for deciding whether a user is allowed to access a service and having:

means for receiving a service authorization request from an Application Gateway Module; and

means for returning to the Application Gateway Module a response on whether the user is granted access to the requested service;

the Authorization Module comprising :

means for generating a service session identifier intended to correlate those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;

means for configuring a second finite-state machine with a number of statuses intended to identify specific events in service progression, the second finite-state machine usable by the Authorization Module to act over the Application Gateway Module to control the service progression;

means for initiating a specific instance of the second finite-state machine, said specific instance being identified by said service session identifier; and

means for determining service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

16. (Rejected) The Authorization Module of claim 15, wherein the means for generating a service session identifier comprise means for including said service session identifier in the response to be returned to the Application Gateway Module on whether the user is granted access to the requested service.

17. (Canceled)

18. (Rejected) The Authorization Module of claim 15, wherein a particular state is associated with a number of service policies within a specific instance of the second finite- state machine, said instance identified by a given service session identifier.

19. (Rejected) The Authorization Module of claim 15, wherein the means for determining service policies comprise means for including in the response towards the Application Gateway Module at least one information element to activate a service

policy within a specific state in the Application Gateway Module, said at least one information element selected from a non-exhaustive list of references and attributes that comprises:

- a number of message field values to match;
- a set of actions to carry out on matching a given message field value ;
- a number of new timer values to run; and
- a number of transactions to supervise.

20. (Rejected) The Authorization Module of claim 19, wherein the means for including in the response towards the Application Gateway Module at least one information element to activate a service policy include means for indicating that this is a global service policy to apply independently of any service delivery in progress.

21. (Rejected) The Authorization Module of claim 16, further comprising means for receiving a notification, from an Application Gateway Module, indicating a specific event detected in service progression.

22. (Rejected) The Authorization Module of claim 16, further comprising means for receiving a request, from an Application Gateway Module, asking for an instruction to proceed with a service progression.

23. (Rejected) The Authorization Module of claim 22, further comprising means for sending towards the Application Gateway Module an instruction selected from: access granted without restriction, another service to substitute a previous service requested, forced logout, and indication of a state transition.

24. (Rejected) The Authorization Module of claim 16, further comprising means for receiving an application message from at least one entity selected from a number of application servers and provisioning systems, the application message including a given service session identifier intended to identify a specific instance of the second finite-state machine in the Authorization Module.

25. (Rejected) A method for authorizing a user of a service network to access a service offered by a service server of a service provider, the user already authenticated by the service network, the server arranged to deliver a service that comprises a plurality of transactions by exchanging a plurality of application messages with the user, the method comprising the steps of:

obtaining a first authorization decision on whether the user is allowed to access the service;

generating and assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;

configuring at least one finite-state machine with a number of statuses intended to identify specific events in service delivery, the finite-state machine usable for controlling service progression

initiating a specific instance of the at least one finite-state machine, said specific instance being identified by the assigned service session identifier; and

activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

26. (Canceled)

27. (Rejected) The method of claim 25, wherein a particular state within the specific instance of the at least one finite-state machine is associated with a number of service policies.

28. (Rejected) The method of claim 25, wherein the step of activating service policies includes a step of setting at least one element selected from a non-exhaustive list of references and attributes that comprises: a number of message field values to match, a number of specific actions to carry out on matching, a number of timer values to run, and a number of transactions to supervise.

29. (Rejected) The method of claim 25, further comprising a step of receiving at the service network an application message originated at an entity selected from: a number of service servers of a service provider and a number of entities of a provisioning system, the application message including a given service session identifier intended to identify a specific instance of the at least one finite-state machine.

30. (Rejected) The method of claim 25, wherein the step of configuring at least one finite-state machine further comprises configuring a first finite-state machine in an Application Gateway Module and configuring a second finite-state machine in an Authorization Module.

31. (Rejected) An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, the Application Gateway Module comprising:

means for obtaining an authorization decision on whether the user is allowed to access the service;

means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;

means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression from a null state, a service authorization state, an active service state, and a disconnect service state; and

means for activating service policies applicable to said specific events and resulting in a state transition in the first finite-state machine, the activating means further comprising:

means for statically arming at least one of the service policies before arrival of a first message to invoke the service; and

means for dynamically arming at least one of the service policies during the progression of the service.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.